Department of Homeland Security Daily Open Source Infrastructure Report for 01 August 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Contra Costa Times reports starting a week ago, problems with overhead transformers and other distribution equipment cut off electricity to millions of Californians, including one out of every five PG&E customers; the outages highlighted the vulnerability of an aging system of cables and equipment. (See item 3)
- The St. Louis Post Dispatch reports eight canines at Lambert Field are helping police to screen every piece of cargo that leaves the airport in passenger planes; Lambert is one of very few airports nationwide to have 100 percent screening of cargo on passenger aircraft. (See item 21)
- The Associated Press reports on Sunday, July 30, New Jersey began a weeklong drill to test how five specialty labs detect bioterrorism agents and how quickly and accurately the state can transmit health−related information during a terror attack. (See item 30)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 31, WNBC 4 (NY)* — **New York heat wave.** New York has begun another heat wave that could last through Wednesday, August 2. Temperatures are expected to hover in the mid−90s.

Even on Thursday, temperatures could be close to 90. The National Weather Service issued heat watches (100 degrees to 105 degrees) and heat warnings (near 105 degrees) for southeastern Pennsylvania and central−southern New Jersey. Con Ed expects record consumption on Tuesday and Wednesday, and has strongly urged energy conservation to avoid another blackout like the recent one in Queens, NY. Con Edison said it has crews working around the clock to repair hundreds of cables that line streets in Astoria, Queens. Thirty−six emergency generators have been bolstering Con Ed equipment while crews do permanent repairs on the cables. The generators are the sole source of power for the time being in areas that have not yet been reconnected to the Con Ed electrical grid. The state's largest utilities said they were prepared to restore power if it goes out.
Source: http://www.msnbc.msn.com/id/14117384/

2. *July 31, Reuters* — **Heat wave to push Midwest power demand to record.** Power grid operators in the Midwest forecast record electricity usage Monday, July 31. The Midwest Independent System Operator, which operates the grid in 15 states and the Canadian province of Manitoba, forecast peak demand would reach 119,396 megawatts (MW) on Monday, breaking the record of 113,054 MW set on July 17. That would be more than six percent over last year's record of 112,197 MW. After temperatures climbed past 100 degrees in some Midwest cities over the weekend, meteorologists forecast highs Monday and Tuesday would reach 94 in Indianapolis, 99 in Chicago, Detroit, and St. Louis, and 101 in Minneapolis. Also over the weekend, electricity traders noted the shut down and power reduction of several of the region's big nuclear power plants, including DTE Energy Co.'s Fermi 2 unit in Michigan and American Electric Power Co. Inc.'s Cook 1 unit in Michigan, would put additional strain on the system. So far, the Midwest ISO has not taken any steps to reduce demand −− no rotating blackouts −− and heat related outages have been relatively minimal. Some 50,000 customer in the Great Lakes region lost power over the weekend due to storms.
Source: http://www.usatoday.com/weather/news/2006−07−31−heat−power_x .htm?csp=34

3. *July 30, Contra Costa Times (CA)* — **Outages identify PG&E's limits.** Starting a week ago, an epidemic of problems with overhead transformers and other distribution equipment cut off electricity to millions of Californians, including one out of every five PG&E customers. Approximately 1,150 of PG&E's 970,000 distribution line transformers failed. The widespread outages highlighted the vulnerability of system of cables and equipment. It also highlighted questions about the adequacy of PG&E's oversight and investment in a system that it already spends more than $400 million a year to operate and more than $800 million to expand and upgrade. Richard Brown, the author of a textbook on electricity distribution systems, said that typically, 80 percent to 90 percent of power outages result from problems in the distribution system. Because those outages occur mostly as scattered events, they remain nearly invisible to the general public. PG&E recently described about 60,000 of its one million overhead and underground transformers as "potentially overloaded." But because of limitations in the method it uses to identify such overloads, PG&E delayed addressing its transformer problems. More than half of the company's substations are at least 50 years old, and a majority of its underground cables are more than 40 years old.
Source: http://www.contracostatimes.com/mld/cctimes/news/local/states/california/15157824.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 31, Foster's Online (NH)* — **Propane leak in New Hampshire prompts evacuations.** Three or four homes were evacuated when propane from an underground tank was released into the air Wednesday morning, July 26, on Boulder Drive, in Barrington, NH. According to Fire Chief Rick Walker, a tree cutting company was in the area, and shortly before 11 a.m. EDT one of its trucks backed over and broke off the top valve of an underground propane tank.
Source: http://www.fosters.com/apps/pbcs.dll/article?AID=/20060731/NEWS05/60731012/−1/NEWS24

5. *July 31, WNDU 16 (IN)* — **Hydrochloric acid leak prompts road closure in Indiana.** A hydrochloric acid leak Monday morning, July 31, at the National Products business in LaPorte County, IN, caused quite a bit of concern. The LaPorte County Sheriff's Department says it was a broken pipe that caused the leak of hydrochloric acid, which produced an acid smell and a small vapor cloud. The main road into the Kingsbury Industrial Park was blocked.
Source: http://www.wndu.com/news/072006/news_51731.php

6. *July 30, Associated Press* — **Fire chief: Lack of fatalities in propane blast an act of grace.** A top fire official said Sunday, July 30, the fact that no one was seriously injured or killed by a series of massive explosions at two propane businesses in North Las Vegas over the weekend was “purely an act of grace.” Chunks of tank weighing about 300 pounds were found as far as 300 yards away after a series of explosions rocked neighboring propane businesses Friday night, said North Las Vegas fire deputy chief Kevin Brame. The explosions were sparked when a man was transferring propane from a large tank to a smaller one, but it was unclear what happened, Brame said. It was not immediately clear if the man was an employee. Residents living as close as 400 yards away from the propane businesses who had been forced to evacuate were allowed to return to their homes at Saturday evening, Brame said.
Source: http://www.signonsandiego.com/news/state/20060730−1646−nv−propaneexplosion.html

7. *July 28, Des Moines Register (IA)* — **Ammonia leak in Iowa prompts evacuations.** The town of Kesley, IA, was evacuated after an anhydrous ammonia leak sprung from a 30,000−gallon tank at the Kesley Ag Center Friday, July 28. Officials said just before they were able to replace the faulty valve on the tank. No injuries were reported.
Source: http://www.desmoinesregister.com/apps/pbcs.dll/article?AID=/20060728/NEWS04/60728014/1001/NEWS

8. *July 26, WALB News (GA)* — **Second chlorine leak in two days prompts evacuations.** One day after a leaking chlorine cylinder was transported from Tifton Aluminum in Tifton, GA, to a gas company called Linde Gas, it sprang a leak again around noon Tuesday, July 25. Firefighters responded to the gas company and evacuated the area.
Source: http://www.walb.com/Global/story.asp?S=5201698&nav=5kZQ

[Return to top]

Defense Industrial Base Sector

9. *July 29, Washington Post* — **Fighting roadside bombs: Low−tech, high−tech, toy box.** After more than three years of war in Iraq, roadside bombs remain the deadliest single threat to U.S. troops, and countering them has emerged as one of the chief technological problems of the conflict. The Pentagon has spent tens of millions of dollars on the most obvious fixes only to see the insurgents develop larger, better concealed and more complicated explosives triggered by cell phones, garage door openers, pressure hoses and other methods. Now, a Pentagon agency with a $3.3 billion budget and a staff of 300 has a mandate to focus the defense industry on the problem. The undertaking has attracted not only the country's top weapons makers but also dozens of small businesses. The defense industry's response to the roadside bomb problem mirrors in some ways the response to the September 11, 2001, terrorist attacks, with many companies establishing internal units to go after the market. So far the threat from the bombs is outrunning the technical creativity of U.S. industry, and the Pentagon now views the bombs as a long−term problem. The search, Pentagon officials say, is not so much for a silver−bullet solution as for a wider set of tools that troops can use.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/28/AR2006072801462.html

[Return to top]

Banking and Finance Sector

10. *July 31, Register (UK)* — **419ers debut Interpol mirror site.** 419 advanced fee scammers have created an exact copy of the Interpol Website, which is expected to be used to dupe victims into believing they are dealing with the real International Criminal Police Organization. A spokesperson for Ultrascan Advanced Global Investigations, a firm which has been studying 419 matters since the mid 90s, says Interpolglobal is "the best scam site we've seen so far." In dealings with potential victims, scammers can now refer to "Interpol" to create an aura of "trust", Ultrascan says, in particular when large sums of money need to be transferred. Although the Interpolglobal site cites the correct address for Interpol in Paris, it lists a different e−mail address. The Website −− registered last December by "Interpol" based in "London, Beijing, GB" −− went up last week, but removing it won't be easy as it is running from a server in China. "419 scammers now include people with PhDs, well capable of creating good looking websites and running them from bullet proof servers," says Frank Engelsman of Ultrascan. The real Interpol has already responded to the new site.
    Source: http://www.channelregister.co.uk/2006/07/31/scammers_create__interpol_mirror/

11. *July 31, Government Computer News* — **GSA warns public of e−mail scam.** The General Services Administration is warning the public about an e−mail scam asking for personal credit card information. The phishing attack is supposedly coming from GSA’s FirstGov.gov portal, fraud@firstgov.gov. It asks the recipient to click on a link for Money Access Online and submit credit card information to confirm the account has not been stolen or hacked. The agency is investigating.
    Source: http://www.gcn.com/online/vol1_no1/41521−1.html

12. *July 30, Websense Security Labs* — **Phishing Alert: First United Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of First United Bank, which is based in Oklahoma. Users receive a spoofed e−mail message claiming that their account has been limited as a result of unusual activity. The e−mail message contains a link to a phishing Website, which attempts to capture the account password, address, and credit card information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =567

13. *July 28, Websense Security Labs* — **Phishing Alert: Bank of Scotland.** Websense Security Labs has received reports of a new phishing attack that targets customers of Bank of Scotland. Users receive a spoofed e−mail message, which claims that a scheduled software update is taking place and user details need to be confirmed. The message provides a link to a phishing Website that requests users to log on and provide account details.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =566

14. *July 28, Federal Financial Institutions Examination Council* — **Agencies release revised Bank Secrecy Act/Anti−Money Laundering Examination manual.** The Federal Financial Institutions Examination Council Friday, July 28, released the revised Bank Secrecy Act/Anti−Money Laundering (BSA/AML) Examination Manual. The revised manual reflects the ongoing commitment of the federal banking agencies and the Financial Crimes Enforcement Network to provide current and consistent guidance on risk−based policies, procedures, and processes for banking organizations to comply with the BSA and safeguard operations from money laundering and terrorist financing. The manual has been updated to further clarify supervisory expectations and incorporate regulatory changes since the manual's 2005 release.
Manual: http://www.ffiec.gov/bsa_aml_infobase/default.htm.
Source: http://www.ffiec.gov/press/pr072806.htm

15. *July 28, Computerworld* — **Banks face Web security deadline.** For some bank IT managers, last fall's release of federal guidelines by the Federal Financial Institutions Examination Council (FFIEC) for validating the identities of online users helped catalyze ongoing efforts to adopt so−called strong authentication measures. But a majority of U.S. banks appear unprepared to meet the December 31 deadline by which they're supposed to comply with the guidelines, several analysts said this week. They placed much of the blame for the current lack of preparedness on the fact that the guidelines aren't mandatory and leave it up to banks to decide what form of strong authentication they should implement. Gartner Inc. analyst Avivah Litan estimated that no more than 20 percent of U.S. banks are in compliance now. "Many banks didn't take this very seriously early on," she said. Litan added, though, that much of the confusion appears to be dissipating as the deadline gets closer and more banks begin to complete their risk assessments and figure out what kind of strengthened authentication approaches they should take.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002085

[Return to top]

Transportation and Border Security Sector

16. *July 31, Oshkosh Northwestern (WI)* — **Runway accident kills Canadian man.** A 63−year−old man from Canada was killed Sunday, July 30, when a Navy warbird's propeller hit a Canadian−registered homebuilt aircraft on a taxiway at Wittman Regional Airport in Oshkosh, WI. A Grumman TBM World War II Navy airplane taxied up behind a homebuilt R.V.6 and as it caught up with the significantly smaller homebuilt, the Grumman's propeller sliced into the R.V.6. The passenger in the side−by−side seat R.V.6 was pronounced dead at the scene while the pilot of the aircraft was not injured, authorities said. Winnebago County Deputy Coroner Chuck Hable said the victim's name would be released following notification of his family. The accident was the second fatal incident on the airport grounds during the one−week AirVenture convention. Clifford and Betty Shaw of Edmonds, WA, died when their Europa XS homebuilt airplane crashed on July 23, while on approach to the east−west runway at Wittman Regional Airport. The National Transportation Safety Board, Federal Aviation Administration, and the Winnebago County Sheriff's Department are investigating the incidents.
Source: http://www.thenorthwestern.com/apps/pbcs.dll/article?AID=/20060731/OSH0101/607310349/1128/OSHnews

17. *July 31, Government Accountability Office* — **GAO−06−795: Transportation Security Administration: Oversight of Explosive Detection Systems Maintenance Contracts Can Be Strengthened (Report).** Mandated to screen all checked baggage by using explosive detection systems at airports by December 31, 2003, the Transportation Security Administration (TSA) has deployed two types of screening equipment: explosive detection systems (EDS), which use computer−aided tomography X−rays to recognize explosives, and explosive trace detection (ETD) systems, which use chemical analysis to detect explosive residues. This report discusses (1) EDS and ETD maintenance costs, (2) factors that played a role in these costs, and (3) the extent to which TSA conducts oversight of maintenance contracts. The Government Accountability Office (GAO) reviewed TSA’s contract files and processes for reviewing contractor cost and performance data. GAO recommends that the Secretary of Homeland Security direct TSA to (1) establish a timeline to close out the contract with Boeing Service Company (Boeing) and report to congressional committees on actions to recover any excessive fees awarded to Boeing, (2) establish a timeline to complete the EDS life−cycle model, and (3) revise policies to require documentation for monitoring EDS and ETD maintenance contracts. The Department of Homeland Security concurred with GAO’s recommendations and described actions TSA had taken or planned to take to implement them.
Highlights: http://www.gao.gov/highlights/d06795high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−795

18. *July 31, Department of Transportation* — **Department of Transportation announces emergency funds to repair damaged roads in 31 states.** More than $685 million is headed to 31 states and U.S. territories to pay for roads and bridges damaged by recent hurricanes, flooding and storms, Acting Department of Transportation Secretary Maria Cino announced on Monday, July 31. The Transportation Department’s Federal Highway Administration (FHWA) will reimburse states for expenses associated with 56 emergency situations. The projects paid for by the funds include reconstructing or replacing damaged highways and bridges, establishing detours, removing debris, and replacing signs, lighting and guardrails. Heavy rainfall and flooding caused much of the road and bridge damage. The program is available to reimburse states for certain costs resulting from natural disasters or other emergencies. A table

listing the date, location, and amount of each emergency relief incident is on this Website. A description of each incident is available by calling the FHWA Office of Public Affairs at 202−366−0660.
Source: http://www.dot.gov/affairs/fhwa1106.htm

19. *July 31, Associated Press* — **Hawaii air prices drop even lower.** Hawaii's newest airline, go! −− which is run by Phoenix−based Mesa Air Group Inc. −− has begun offering $29 one−way trips between Honolulu and the Neighbor Islands. That's a $10 drop from the $39 fares currently offered. Both Hawaiian and Aloha airlines say they will match the new fare. The new prices will be valid on tickets purchased by Tuesday, August 1, for travel completed before September 30. The offer is good for travel between Honolulu and Hilo, Kailua−Kona, Lihue, and Hakului. One−way flights between the Neighbor Islands will cost $58. The long−term viability of these fares was questioned after Jonathan Ornstein, Mesa's chairman and chief executive, recently said the company is losing $300 per flight at its $39 rate. But go! wants to solidify its place in the Hawaii air market, and it plans to make money when it brings in larger regional jets next year, company officials say.
Source: http://www.usatoday.com/travel/flights/2006−07−31−hawaii−air fare_x.htm

20. *July 27, Department of Transportation* — **Department of Transportation approves certificate for Eclipse 500.** A new fleet of small−sized jet aircraft are closer to changing the way thousands of travelers fly now that the Department of Transportation's Federal Aviation Administration has granted Eclipse Aviation's new Eclipse 500 aircraft a Provisional Type Certificate. "Thousands of new jets like this are going to redefine the way Americans travel, help cut airport congestion, and drive economic growth in cities and towns across the country that today only dream of commercial air service," Acting Secretary of Transportation Maria Cino said. Cino noted that jets like the Eclipse 500, which are referred to as very light jets, will be able to affordably fly travelers from thousands of small airports across the country because they need less room to land and take off. As a result, she said these new jets will help reduce congestion and cut delays at major airports by giving travelers new options for getting from one small city to the next.
Source: http://www.dot.gov/affairs/dot8106.htm

21. *July 27, St. Louis Post Dispatch* — **Bomb−sniffing dogs at Lambert screen all cargo traveling in passenger planes.** Airline passengers have scrambled for years to remove their shoes, overcoats and belt buckles at the metal detectors, while the cargo beneath them has oftentimes gone unscreened. Now eight canines at Lambert Field in St. Louis are helping police screen every piece of cargo that leaves the airport in passenger planes, Lambert officials said Wednesday, July 26. Lambert will get two more bomb−sniffing canines in September. The airport hit the 100 percent screening mark in April after Airport Police Chief Paul Mason required Lambert's bomb−sniffing dogs to spend more time screening cargo and watching cargo areas. Lambert is one of very few airports nationwide to have 100 percent screening of cargo on passenger aircraft. The Transportation Security Administration does not require it. Last November, the Government Accountability Office reported that the 23 billion pounds of cargo shipped by air every year was barely being checked. All cargo shipped on passenger flights must be handled by companies that are "known shippers," meaning they have security programs that meet transportation safety agency guidelines. This spring, the security agency also required background checks of 51,000 off−airport freight forwarder employees.

Source: http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscityco unty/story/8FFE28DED282A29C862571B80013808D?OpenDocument&highlight=2%2C%22Lambert%22+AND+%22security%22

22. *July 25, Seattle Times* — **Piercing port security as easy as hitching a ride.** Ever since 9/11, U.S. seaports have been preparing for an attack. Fences are up, cameras and lights are on, and a national computer system is crunching data on all cargo coming into the U.S. on ships. But many ports appear to have left at least one gaping hole in their security: simply by riding along with truck drivers to drop off and pick up cargo, an investigative reporter for the Seattle Times easily penetrated the security of ports in Los Angeles−Long Beach and Seattle, two of the nation's largest port complexes. In the only instance where identification was sought, flashing an expired driver's license was all it took before a uniformed guard waved the truck and reporter through the gate. Port officials nationwide know about this lapse in security and say they are doing what they can. A new federal driver−identification system is planned over the next two years as one effort to secure "the land side." Most ports lease their docks to private companies. Those tenants −− the terminal operators −− develop their own security plans, which are approved by the Coast Guard, the agency with overall security responsibility for port facilities.
Source: http://seattletimes.nwsource.com/html/localnews/2003149964_portsecurity25.html

[Return to top]

Postal and Shipping Sector

23. *July 27, HOI 9 (IL)* — **Illinois post office plans for possible disaster.** A "what if" scenario was put in place Thursday afternoon, July 27, at the Peoria, IL, post office on State Street. The drill included an evacuation and biohazard detection system response exercise. It was all in an effort to develop plans to protect employees. Post office officials said it's planning like this that can save lives when emergencies happen. "Security at the postal service and all around the country has stepped up and we always want to make sure safety is in the forefront along with security," said Brian Wagner of the Peoria post office Just in the last year, post office processing and distribution centers, including facilities in Peoria, have been installed with the new biohazard detection system. The system looks for viruses during the mechanical sorting process.
Source: http://www.hoinews.com/news/news_story.aspx?id=13822

[Return to top]

Agriculture Sector

24. *July 31, USAgNet* — **California's cattle death toll surpasses 25,000.** A heat wave baking California since mid July has killed more than 25,000 cattle and 700,000 fowl, prompting emergency measures and crippling the sector for months to come. According to the California Dairy Campaign, the losses amount to 1,500 to 2,500 dollars per head. And milk production in central California is also down. Tulare−based Land O' Lakes Creamery normally produces 1.6 million gallons of milk daily. The company has been reporting losses of 400,000 gallons a day.

The heat also decreases the breeding success of the livestock.
Source: http://www.usagnet.com/story−national.php?Id=1479&yr=2006

25. *July 30, Associated Press* — **Investigation of disease center delayed.** The investigation into waste disposal policies at the National Animal Disease Center in Ames, IA, which was slated to start in June, has yet to begin. Ames water and pollution control director Tom Neumann said a law defining how investigations of federal agencies must occur led to the delay. Neumann said the investigation is now scheduled to begin in mid−to−late August. A team of experts was formed to look into claims from animal caretakers that the lab's waste disposal practices don't effectively deactivate prions, the misshapen proteins blamed for some deadly diseases in humans and animals.
Source: http://abcnews.go.com/Health/wireStory?id=2254880

[Return to top]

Food Sector

26. *July 31, AgProfessional* — **Smithfield Foods to buy ConAgra's refrigerated meats businesses.** Smithfield Foods Inc. and ConAgra Foods Inc. announced Monday, July 31, the signing of a definitive agreement for Smithfield to acquire substantially all of the assets of ConAgra's branded meats business for $575 million. The business includes the packaged meats and turkey products sold under the Armour, Butterball, Eckrich, Margherita, Longmont and LunchMakers brands. The brands are marketed to retail grocers, delis, restaurants and other foodservice establishments. The combined annual sales of the businesses are about $1.8 billion. Smithfield intends to separate the Butterball turkey business from the non−turkey packaged meats business and acquire and operate the Butterball turkey business through Carolina Turkeys, an existing partnership between Smithfield Foods and Maxwell Farms, Inc. Smithfield owns 49 percent of Carolina Turkeys, the fourth largest turkey producer in the U.S. ConAgra confirmed that it will retain the Hebrew National brand and products, Brown 'N Serve frozen sausage, as well as its Slim Jim and Pemmican meat snacks.
Source: http://www.agprofessional.com/show_story.php?id=42217

27. *July 28, Associated Press* — **Mad cow disease interrupts plans to boost imports from Canada.** The Bush administration halted plans to increase imports of beef and cattle from Canada amid new evidence that Canada's safeguards against mad cow disease are not working. The Bush administration had been poised to expand beef trade with Canada, but the U.S. Department of Agriculture said Friday, July 28, the plan is on hold while Canada investigates a recently discovered case of mad cow disease. At issue is a ban on using cattle remains in cattle feed, the primary firewall against the spread of mad cow disease. The only known way for cattle to get the disease is by eating feed containing diseased cattle tissue, a practice largely outlawed in Canada and the U.S. in 1997. Earlier this month, Canada discovered an infected cow born in 2002, five years after the ban went into effect. The cow's age −− younger than previously infected animals −− suggests a shorter incubation period for the brain wasting disease, meaning it could have gotten a bigger dose of infection than other Canadian cases.
Source: http://www.grandforks.com/mld/grandforks/15147977.htm

28. *July 27, Computing* — **UK food agency beefs up site for peak demand.** The United Kingdom's Food Standards Agency (FSA) is using a utility computing model to ensure its Website stays operational during a major food scare. The technology, which consists of hosted network, storage, and computer architecture, is allowing the independent government department to rapidly increase bandwidth as demand increases, and to deal with spikes in Web traffic automatically. The FSA is also establishing a disaster recovery center in the U.S. to ensure continued service in the event of a major incident in the United Kingdom.
Source: http://www.computing.co.uk/computing/news/2161217/food−agenc y−beefs−site−peak

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

29. *July 31, Washington Post* — **Custom−built pathogens raise bioterror fears.** In 2002, Eckard Wimmer, a molecular geneticist, startled the scientific world by creating the first live, fully artificial virus in the lab. The virus was made wholly from nonliving parts, using equipment and chemicals on hand in Wimmer's laboratory at the State University of New York. The genetic code was picked up on the Internet. Hundreds of bits of viral DNA were purchased online, with final assembly in the lab. Wimmer intended to sound a warning, to show that science had crossed a threshold into an era in which genetically altered and made−from−scratch germ weapons were feasible. But in the four years since, other scientists have made advances faster than Wimmer imagined possible. Government officials and scientists are only beginning to grasp the implications. While government scientists press their search for new drugs for old foes such as anthrax, a revolution in biology has ushered in an age of engineered microbes and novel ways to make them. Today, in hundreds of labs worldwide, it is possible to transform common intestinal microbes into killers. Or to make deadly strains even more lethal. Or to resurrect bygone killers, such the 1918 influenza. Or to craft cheap, efficient delivery systems that can infect large numbers of people.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07 /30/AR2006073000580.html

30. *July 29, Associated Press* — **Bioterror drill to test five labs.** New Jersey on Sunday, July 30, began a weeklong drill to test how five specialty labs detect bioterrorism agents and how quickly and accurately the state can transmit health−related information during a terror attack. Sponsored by the Health and Senior Services Department, the drill will look at five labs in the state to test patient samples, communication with state agencies, shipping and transporting specimens, state confirmation testing and communication back to the labs, said department spokesperson Tom Slater. Patients will not be involved in the exercise, which involves five hospital−based labs. In an actual terrorist attack, specimens would be taken from emergency room patients and tested in the hospital lab. Those labs would be the first to spot suspicious samples or identify possible biologic links. The hospital−based labs participating in the drill are

AtlantiCare Regional Medical Center in Atlantic City; Barnert Hospital in Paterson; Holy Name Hospital in Teaneck, and Robert Wood Johnson University Hospital at Hamilton and New Brunswick.
Source: http://www.philly.com/mld/inquirer/news/local/15149542.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *July 31, Hartford Courant (CT)* — **Connecticut emergency responders pass first big test of regional plan.** Connecticut's Regional Emergency Deployment Plan was the picture of success in its first large−scale test, officials said last week. The Red Plan, as it's called, is used for 20 different types of emergencies, ranging from public health issues to massive power interruptions, situations involving planes, trains, motor vehicles, buildings, hospitals, law enforcement, fires, natural disasters and terrorist attacks. "It was one of the first times it got activated to this level for a fire emergency, and it went like clockwork," Fire Chief Gary F. Ruggiero said. The Red Plan was developed through the Capitol Region Council of Governments to help 42 communities in the Hartford area. The only glitch reported in the entire effort involved communications, because the various groups had their own individual radio channels. "We had to rely on runners, but the state is working on the problem. Our goal is to have 'stock channels,' so everyone communicates better," according to Ruggiero.
Source: http://www.courant.com/news/local/hc−regforce0730.artjul31,0,5416638.story?coll=hc−headlines−local

32. *July 31, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: A tropical wave is located about 425 miles east of the Windward Islands moving west−northwestward at 15−20 mph. This system does not appear to be organizing into a tropical depression. Eastern Pacific: Both Daniel and Emilia lost all tropical characteristics Friday, July 28, so there are no tropical systems in the Eastern Pacific at the current time. An area of low pressure, however, centered about 750 miles south−southwest of the southern tip of Baja, CA, will need to be watched for potential development over the next couple of days. Wildfire Update: Wildland fire activity was light nationally with 151 new fires reported. Twelve new large fires were reported: one each in Arizona, Colorado, Oklahoma, Idaho, Nebraska, North Dakota, Montana, and Utah; and two each in South Dakota and California. To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat073106.shtm

33. *July 27, Department of Homeland Security* — **DHS strengthens intelligence sharing at state and local Fusion Centers.** The Department of Homeland Security (DHS) announced Thursday, July 27, that analysts from the Office of Intelligence and Analysis will work along side state

and local authorities at Fusion Centers in New York City, Los Angeles, Reisterstown, MD, and Baton Rouge, LA. These analysts will help to facilitate the two−way flow of timely, accurate, actionable information on all types of hazards. State and local authorities have created 38 Fusion Centers around the country that blend relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities.
Source: http://www.dhs.gov/dhspublic/display?content=5760

[Return to top]

Information Technology and Telecommunications Sector

34. *July 31, Sophos* — **Top ten malware threats and hoaxes reported to Sophos in July 2006.** Sophos has revealed the most prevalent malware threats and hoaxes causing problems for computer users around the world during July 2006. The information reveals that while the Netsky−P worm, first seen in March 2004, remains the most widespread piece of malware traveling via e−mail, the actual proportion of infected e−mail has dropped to a low of just one in 222 (0.45 percent). This compares to the first six months of 2006 when, on average, one in 91 e−mails (1.1 percent) carried malicious attachments. Sophos identified 3,715 new threats in July, bringing the total of malware protected against to 184,007. The majority of the new threats (87 percent) were Trojan horses, while just 13 percent were worms or viruses. See source for full report.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/top−ten−virus−report−july−2006.html

35. *July 30, Government Accountability Office* — **GAO−06−675: Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain (Report).** The Internet protocol (IP) provides the addressing mechanism that defines how and where information such as text, voice, music, and video move across interconnected networks. IP version 4 may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. As a result, Internet version 6 (IPv6) was developed to increase the amount of available address space. In August 2005, the Office of Management and Budget (OMB) issued a memorandum specifying activities and time frames for federal agencies to transition to IPv6. The Government Accountability Office (GAO) was asked to determine (1) the status of federal agencies' efforts to transition to IPv6; (2) what emerging applications are being planned or implemented that take advantage of IPv6 features; and (3) key challenges industry and government agencies face as they transition to the new protocol. GAO recommends that federal agencies work through two of the groups that play key roles in transitioning the federal government to IPv6 to address key challenges they face as they proceed with the transition. In oral comments on a draft of this report, OMB generally agreed with the results.
Highlights: http://www.gao.gov/highlights/d06675high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−675

36. *July 28, Secunia* — **Symantec Brightmail AntiSpam multiple vulnerabilities.** Some vulnerabilities have been reported in Symantec Brightmail AntiSpam, which can be exploited to cause a denial−of−service and overwrite or read sensitive information. Analysis: 1) When installing e−mail scanners, it is possible to select an option that allows the Control Center to

connect from any computer. If this option is selected, it is possible to impersonate the Control Center and cause the Brightmail AntiSpam service to stop responding by sending invalid posts. 2) Input passed in "DATABLOB−GET" and "DATABLOB−SAVE" requests is not properly sanitized. This can be exploited to overwrite or read some files on the system in combination with vulnerability #1.
Vulnerable: Symantec Brightmail AntiSpam 4.x; Symantec Brightmail AntiSpam 5.x; Symantec Brightmail AntiSpam 6.x.
Solution: Update to version 6.0.4 or upgrade to Symantec Mail Security for SMTP 5.0.
Source: http://secunia.com/advisories/21223/

37. *July 28, IDG News Service* — **Microsoft to charge for Office 2007 beta 2.** Microsoft said on Friday, July 28, that it will begin charging $1.50 for users to download a copy of the Office 2007 beta 2 Wednesday, August 2. "Given how dramatically the beta 2 downloads have exceeded our goals, we have made the business decision to implement a cost−recovery measure for downloading the beta," the company said.
Source: http://www.infoworld.com/article/06/07/28/HNoffice2007betafe e_1.html

38. *July 28, Sophos* — **"My best photo ever!" Trojan horse spammed out via e−mail.** Sophos has warned of a Trojan horse that has been spammed out to e−mail addresses disguised as a digital photograph. The Troj/Dloadr−AKX Trojan horse has a subject line with one of the following text: "My best photos!"; "the best pictures of us. Just take a look, i'm excited!"; "Wanna see?"; or "You've asked for pictures. See this." The attached file is photos.zip. Inside the ZIP file is another file called DSC00342.jpg .exe. The executable file is a Trojan horse designed to download further malicious code from the Internet, but disguises itself as a JPG graphic by using a double extension and inserting multiple spaces into the filename.
Source: http://www.sophos.com/pressoffice/news/articles/2006/07/dloa dr−kx−trojan.html

39. *July 27, Search Security* — **DHS puts Zitz in charge of cybersecurity division.** The U.S. Department of Homeland Security (DHS) has found someone to take over the daily responsibility of running the National Cyber Security Division (NCSD). But the department has yet to fill the vacant post of assistant secretary for cyber security and telecommunication. Robert S. Zitz, the deputy undersecretary for preparedness at DHS, has been tapped to oversee the day−to−day operations of the NCSD. Andy Purdy, the acting director of the NCSD, whose contract with DHS ends in October, will remain in place but Zitz now will be spending a portion of his time working with him and the rest of the NCSD senior staff. Zitz will continue to report to George Foresman, the under secretary for preparedness, who oversees the branch of DHS that includes the NCSD. Jarrod Agen, a spokesperson for DHS, said Zitz will maintain his other duties and will not take over the assistant secretary job, which has remain unfilled since DHS Secretary Michael Chertoff created it last July. However, Agen said, the department is "close to the final stages of hiring someone" for the assistant secretary position.
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1205259,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received information that a website on the Internet is hosting malicious software that has been or is currently being used to compromise systems.

IP: 211.34.248.244

Activity:
This activity is similar to what was reported on July 6th concerning the "beststartmotor" domain. The original email stated: "In April 2006, users reported having their web browsers redirected from other websites to the domain beststartmotor.com using an HTML command called an iframe. Once redirected, the victim's web browsers usually download malware onto the victim's computer." Currently, another website may have a similar iframe link to IP 211.34.248.244. Once a web browser on a victim system follows this link, the victim computer may download malware which can compromise that computer.

Recommendation:
US−CERT suggests that each agency evaluate the potential risk and take protective measures in a manner that is consistent with the agency's policies and procedures. Please refrain from investigating / visiting the IP address as this may result in accidental infection of your computer. Please be advised that the IP address listed above may also host additional domains and websites. However, this information is being shared to allow the GFIRST community to understand the potential risk associated with those domains.

US−CERT requests that all agencies examine firewall, web proxy and other network perimeter device logs for suspicious traffic to and from the above IP. Should you encounter such activity, please notify US−CERT at soc@us−cert.gov or via phone at 888−282−0870.

Active Exploitation of a Vulnerability in Microsoft PowerPoint
US−CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

VU#936945: Microsoft PowerPoint contains an unspecified remote code execution vulnerability. http://www.kb.cert.org/vuls/id/936945

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read

Cyber Security Tip ST04−010 for more information on working with email attachments. http://www.us−cert.gov/cas/tips/ST04−010.html

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 445 (microsoft−ds), 139 (netbios−ssn), 135 (epmap), 113 (auth), 41170 (−−−), 80 (www), 6346 (gnutella−svc), 1025 (win−rpc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *July 29, Times−Tribune (PA)* — **Pennsylvania school district to install security system.** The Pittston School Board will install a $265,000, state−of−the−art surveillance system inside and outside all five of the Pennsylvania school district's buildings. The high−tech system is part of a $7 million high school renovation project that could begin by next summer, said school district Superintendent Ross Scarantino. The system will include about 60 surveillance cameras, monitors at a control center in the high school and swipe cards for employees. "There's a lot of (vandalism) damage in the schools, especially in the middle school," said board member Joseph Oliveri, chairman of the security committee. The cameras would scan hallways and outside the schools, including the bus ports. The cameras, which will have night vision, would not only detect and record vandalism at the schools after hours, they might help prevent a Columbine−type incident in the schools, said Oliveri, referring to the horrific 1999 incident at Columbine High School in Colorado. Oliveri is hoping the district can obtain grants from the U.S. Department of Homeland Security or the Pennsylvania Commission on Crime and Delinquency.
Source: http://www.thetimes−tribune.com/site/news.cfm?newsid=16983354&BRD=2185&PAG=461&dept_id=416046&rfi=6

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer